SEC MEMORANDUM CIRCULAR NO. 23
Series of 2026

TO	:	**ALL CONCERNED CORPORATIONS**
SUBJECT	:	**BLOCKCHAIN-BASED DIGITAL SIGNING AND AUTHENTICATION OF SEC-RELATED DOCUMENTS USING THE SEC VERITAS**

WHEREAS, the Commission is mandated under Section 180 of Republic Act No. 11232, otherwise known as the Revised Corporation Code of the Philippines (RCC), to develop and implement an electronic filing and monitoring system to facilitate and expedite corporate name reservation and registration, incorporation, submission of reports, notices, and other documents required under the Code, and to promulgate rules and regulations to carry out these functions;

WHEREAS, Section 179 (o) of the RCC grants the Commission the power and authority to formulate and enforce standards, guidelines, policies, rules, and regulations necessary to implement the provisions of the Code, including the adoption of digital systems and authentication mechanisms;

WHEREAS, the Commission issued Memorandum Circular (MC) No. 10, Series of 2024, on the Electronic SEC Universal Registration Environment (eSECURE), which establishes a centralized digital identity and credentialing system for individuals transacting with the Commission, enabling risk-based electronic Know Your Customer (eKYC) procedures and digital authentication of documents through the Electronic Submission Authentication Portal (eSAP);

WHEREAS, the eSECURE system allows credentialed users to digitally authenticate submissions without the need for wet signatures or notarization, in compliance with Republic Act No. 8792, otherwise known as the Electronic Commerce Act (ECA), which recognizes the legal validity of electronic signatures and documents;

WHEREAS, the implementation of eSECURE supports the objectives of Republic Act No. 11032, otherwise known as the Ease of Doing Business and Efficient Government Service Delivery Act of 2018 (EDBA), by streamlining regulatory processes, reducing transaction time, and enhancing the efficiency and accessibility of government services;

WHEREAS, Section 9(e) of EDBA necessitates government agencies, when applicable, to develop electronic versions of licenses, clearances, permits, certifications, or authorizations with the same level of authority as that of the signed hard copy, which may be printed by the applicants or requesting parties in the convenience of their offices;

WHEREAS, the Philippine Development Plan (PDP) 2023–2028, particularly under Chapter 10 entitled "*Promote Competition and Improve Regulatory Efficiency*" calls to expedite efforts to streamline processes for business registration. Meanwhile, Chapter 14 thereof, entitled "*Practice Good Governance and Improve Bureaucratic Efficiency*" emphasizes the need to accelerate digital transformation specifically the adoption of interoperable, secure, and paperless transactions;

WHEREAS, in line with the PDP, the integration of secure digital authentication across government agencies through the adoption of advanced technologies like blockchain, will enhance the integrity and verifiability of electronic submissions;

WHEREAS, blockchain technology offers a decentralized, tamper-evident, and cryptographically secure method of recording transactions, enabling the creation of immutable audit trails through the use of cryptographic hashing and timestamping, thereby reinforcing the principles of authentication, integrity, and non-repudiation in digital signatures;

WHEREAS, the Commission has developed the Verification of Electronic Records and Information Trust and Authentication System (VERITAS), a blockchain-based document signing and verification platform designed to strengthen the security, reliability, and non-repudiation of digitally signed and authenticated submissions; and

Published on:
Philippine Star, 28 July 2026
Manila Bulletin, 28 July 2026

Filed with UP Law Center:
27 July 2026

WHEREAS, the integration of VERITAS into the eSECURE and eSAP platforms represents a forward-looking enhancement that aligns with global best practices in digital governance and supports the Commission's commitment to regulatory innovation, fraud prevention, and investor protection;

NOW, THEREFORE, the Commission, pursuant to its mandate to modernize its regulatory framework and in support of national development goals, hereby issues and promulgates the following guidelines for the use of blockchain-based digital signing and authentication through VERITAS.

Section 1. Definition of Terms

For the purposes of this Circular, the following terms are defined as follows:

1.1. **SEC Check App** is the official mobile application of the Commission that is available for download in Apple Appstore and Google Play.

1.2. **VERITAS** refers to the Verification of Electronic Records and Information Trust and Authentication System, the Commission's blockchain-based document signing and verification platform. It is available in the SEC Check App.

1.3. **eSECURE** means the Electronic SEC Universal Registration Environment, the Commission's digital identity and credentialing system.

1.4. **eSAP** means the Electronic Submission Authentication Portal used for digital authentication of SEC documents.

1.5. **Digital Signature** is synonymous with "Digital Signature" as defined under A.M. No. 01-7-01-SC, or the Rules on Electronic Evidence, and refers to an electronic signature consisting of a transformation of an electronic document using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer's public key can accurately determine (i) whether the transformation was created using the private key that corresponds to the signer's public key; and (ii) whether the initial electronic document had been altered after the transformation was made.

1.6. **Document** means an electronic file, typically in PDF format, submitted to the Commission for authentication.

1.7. **Signing** means the act of attaching or logically associating a user's Digital Signature with a document through VERITAS.

1.8. **Blockchain** means the decentralized ledger technology used to record document signing events in VERITAS, ensuring immutability and verifiability.

1.9. **Private Key** means the confidential cryptographic key owned and controlled by a user to sign documents, also referred to as the Document Signing Certificate.

1.10. **Public Key** means the cryptographic key used to verify digital signatures.

1.11. **Document Signing Certificate** means the user's private key used to sign documents in VERITAS.

1.12. **Cryptographic Hash** means a unique digital fingerprint of a document generated through a secure algorithm such that any alteration results in a different hash.

1.13. **PNPKI** is the Philippine National Public Key Infrastructure, managed by the Department of Information and Communications Technology (DICT), used for digital certificate.

1.14. **Passphrase** is a sequence of words used for authentication, similar to a password, but is typically longer and harder to guess, providing enhanced security for accounts and data.

Section 2. Scope

This Memorandum Circular applies to all individuals with a credentialed eSECURE account, including incorporators, directors, officers, authorized representatives, and other persons who are designated to sign and submit documents to the Commission on behalf of a juridical entity. It covers all corporations, partnerships, and other juridical entities registered with the Commission as well as Commission departments, extension offices, and personnel involved in the processing, verification, and archiving of electronically submitted documents.

Section 3. Use of VERITAS for Blockchain-based Digital Signature and Authentication

3.1. The VERITAS shall enable users with installed SEC Check App on mobile devices and credentialed eSECURE accounts to securely sign and verify SEC-related documents using public-key cryptography. It shall record digital signing events on a decentralized ledger, ensuring immutability, timestamping, and cryptographic verification, thereby reinforcing the principles of authentication, integrity, and non-repudiation in electronic transactions.

3.2. The VERITAS shall operate as a secure digital signature platform that employs end-to-end encryption, multi-factor authentication, and cryptographic signing mechanisms using the user's Document Signing Certificate, ensuring that only authorized individuals can sign documents. The platform shall be designed to prevent unauthorized access, tampering, or forgery, and shall be regularly audited for compliance with cybersecurity standards.

3.3. Only digital signing certificates and public-private keypairs generated and issued by the VERITAS on-chain shall be used to sign documents within the platform. The use of externally issued digital certificates and public-private keypairs, including those issued by Commercial Certificate Authorities, is not allowed under the current operational policy of the platform.

3.4. The VERITAS shall ensure the proper authentication of the signer's identity. No individual may execute a digital signature through VERITAS without first possessing a valid and active credentialed eSECURE account. The credentialing process, which constitutes an eKYC procedure, requires the submission of verified government-issued identification documents and the completion of a liveness detection protocol. This process establishes a reliable and verifiable link between the digital signature and the legal identity of the signatory.

3.5. The VERITAS shall ensure the integrity of the document throughout the signing process.

3.5.1. Upon initial upload, each document shall be subjected to a cryptographic hashing algorithm, generating a unique digital fingerprint of its content. This hash shall then be digitally signed using the user's private key, and appended to the blockchain used by VERITAS, together with an encrypted list of required/authorized signatories.

3.5.2. Each authorized signatory shall review and modify the document to add signature appearances. The modified document shall be subjected to a cryptographic hashing algorithm, at which point its hash shall then be digitally signed with the authorized signatory's private key and appended to the blockchain.

3.5.3. Once all authorized signatories have signed the document, SEC shall attach a visible DICT-issued PNPKI Agency Certificate seal and a Quick Response (QR) code to each page. The QR code shall allow users to view the final document, ensuring that the document remains tamper-evident and unaltered from the point of execution. This final document's hash shall be signed by SEC's private key and appended to the blockchain.

3.5.4. At the end of the signing process, the hashes of all versions of the document, including the originally uploaded document, each signed version, and the final document that contains the QR code of SEC, which is signed by the DICT-issued PNPKI Agency Certification of the SEC and counter-signed by its private key, shall all be stored on the blockchain. Any alteration to any version of the signed document shall be readily detectable through a mismatch between the

hash of the altered document and the corresponding hash of those immutably stored on the blockchain.

3.6. The VERITAS shall maintain a detailed and immutable audit trail of every document submission and signing transaction. This shall include the encrypted identity of each authorized signer, the date and time of signing, the Internet Protocol (IP) address used, and the signing transaction number. This audit log shall be permanently recorded on the blockchain used by the VERITAS, providing an immutable and verifiable record that can serve as conclusive evidence of the authenticity, integrity, and non-repudiation of the digital signature.

3.7. Documents eligible for signing and authentication through VERITAS shall include, but shall not be limited to:

3.7.1. Articles of Incorporation and By-Laws;
3.7.2. Certificates of Authentication; and
3.7.3. Any other document that requires, or may in the future require, digital authentication under SEC rules.

Section 4. Acceptance and Verification of Digitally Signed and Authenticated Documents Through VERITAS

4.1. Documents digitally signed and authenticated through VERITAS shall be accepted as duly signed and authentic copies **for purposes of SEC transactions**. Pursuant to ECA, such documents shall have the same legal effect and enforceability as a signed and notarized written document, **unless a specific provision of law explicitly requires notarization or another form of authentication**.

4.2. The digital version of the document shall be considered the official and original record, and the submission of hard copies of VERITAS-signed documents shall no longer be required, subject to laws and other rules implemented by the Commission that still require the submission of physical copies of documents. Printouts or paper reproductions of digitally authenticated documents shall be considered duplicates or secondary copies and shall have a notation or disclosure that shall read, "*The original of this document is in digital format,*" or other similar language.

4.3. The authenticity of a VERITAS-signed and authenticated document shall be verified by uploading the digital copy of the document to the document verification module of the VERITAS or the eSAP. Upon submission, the system shall indicate whether the document is verified to be valid and authentic. In cases where the document cannot be validated, the system shall notify the user of its invalidity and provide the grounds therefore, which may include any of the following:

- The document is not found in the blockchain used by the VERITAS;
- The digital signatures affixed to the document are incomplete;
- The document is not signed using the PNPKI digital certificate of the SEC; or
- The document does not contain valid and legitimate details (e.g., eSAP QR code), as assessed by eSAP.

4.4. Documents signed through VERITAS shall remain subject to post-evaluation, audit, compliance verification, and legal review by the Commission. The Commission reserves the right to withhold recognition of any such document should it be found non-compliant with applicable laws, rules, or regulations, or if the integrity of the signing process is deemed to have been compromised.

Section 5. User Responsibilities and Security

5.1. Users shall be solely responsible for the security and integrity of their digital identities and transactions in VERITAS. Specifically, users shall:

- Safeguard their Document Signing Certificate and ensure it is not shared, lost, or compromised;
- Back up the Document Signing Certificate to ensure that it can be restored in case the

VERITAS-enabled device is lost or replaced;

- Recover access to the Document Signing Certificate in case of lost Document Signing Certificate QR code backup or forgotten QR code passphrase through the established social recovery mechanism;
- Secure their VERITAS-enabled devices, including the passphrase and QR code associated with the account;
- Ensure the accuracy and completeness of documents before signing;
- Use VERITAS only for SEC-related documents;
- Refrain from uploading or signing fraudulent, illegal, or unauthorized documents; and
- Refrain from using VERITAS for any activity that violates data protection, anti-fraud, or anti-money laundering laws.

5.2. The Commission shall not have access to, nor be able to recover, lost or compromised private keys. Furthermore, the system does not store private keys and personal information beyond what is required for cryptographic verification. Any unauthorized use resulting from negligence in safeguarding the private key shall be the sole responsibility of the user.

5.3. Transactions recorded on the blockchain used by VERITAS are permanent and immutable. Once a document is signed and recorded, it cannot be altered or deleted. If amendments, supplements or corrections are needed, the user shall restart the submission and signing process with a revised document. In case of revisions, the latest submitted document shall be presumed as the official document filed.

Section 6. Administrative Sanctions

6.1. Any individual or entity found to have tampered with a blockchain record, misused digital credentials, or submitted falsified documents shall be denied access to the eSECURE, and all the corresponding privileges attached to such access shall be suspended. The case may also be referred to the other operating departments of the Commission for investigation and imposition of applicable administrative sanctions.

6.2. The Commission shall not be precluded to refer the case to appropriate government agencies for possible prosecution under applicable laws, including ECA, Republic Act No. 10173, otherwise known as the Data Privacy Act (DPA), and Act 3815, otherwise known as the Revised Penal Code.

Section 7. No Fee Due

The use of VERITAS shall be provided free of charge; Provided, however, that the Commission reserves the right to impose reasonable fees, through an appropriate issuance, as may be necessary to defray costs associated with the system network infrastructure and application services.

Section 8. VERITAS User Guide, System Availability and Technical Support

Except for scheduled system maintenance, VERITAS shall be available and accessible 24 hours a day, seven days a week. However, the system is provided on "as is" and "as available" basis, with no guarantee of uninterrupted service. Access to the system may be temporarily impaired due to downtime, maintenance, network disruptions, or the user's internet service conditions.

8.1 The complete VERITAS User Guide shall be available for viewing and downloading online at the eSAP and the SEC Check App for reference. The Commission expressly reserves the right to update or modify the service at its sole discretion and without prior notice.

8.2 For inquiries, clarifications and/or technical concerns on the use of VERITAS, users may contact the technical support of the Information and Communications Technology Department (ICTD) by using the iMessage portal (https://imessage.sec.gov.ph). The technical support shall be available from 8:00 a.m. to 5:00 p.m. during workdays.

8.3 System integration and procedural issues such as but not limited to resolving discrepancies in the validation/non-validation of VERITAS-signed reports/documents, shall be addressed in the VERITAS User Guide.

8.4 Deadline adjustments due to system downtime shall be disseminated through separate

advisories or issuances as may be necessary.

Section 9. Modification or Amendment

The provisions herein amend and supplement Section 6 of SEC MC No. 10, Series of 2024, and shall govern the use of VERITAS for digital signing and authentication in conjunction with the eSECURE platform and other integrated online systems of the Commission.

Section 10. Implementation

The use of VERITAS for the digital signing and authentication of documents shall be optional, and the existing PNPKI-based digital authentication via the eSAP shall remain available and operational.

Through an appropriate issuance, and after the necessary public consultation, the Commission may require the mandatory implementation of the VERITAS for specific types of filings or entities.

Section 11. Effectivity

This Memorandum Circular shall take effect immediately after publication in two (2) newspapers of general circulation in the Philippines.

Makati City, Philippines, July 27, 2026.

For the Commission:

FRANCISCO ED. LIM
Chairperson